Overview of Operational, Security, Privacy Practices and Compliance Frameworks

QHR Technologies Inc. has been providing professional electronic medical record systems to Canadian health care professionals since 2004. The health records of over 5,000 organizations in Canada are hosted in QHR's data centers, or with our cloud providers. These organizations range from single practitioners to enterprise clinics with over 100 medical professionals.

Purpose

This document provides an overview of key operational, security, and privacy-related questions that are commonly asked of QHR. This document is general in nature and does not supersede nor alter in any way your contractual agreement(s) with QHR. This document is subject to change without notice.

Table of Contents

1. Security

QHR follows a defense-in-depth strategy. In simple terms: we make use of overlapping and redundant security measures so that if one measure is overcome, other measures will still provide protection.

a. Access Controls

- **QHR Employee Access**
    - Multi-factor authentication (MFA) is required for all employee logins to QHR assets. QHR has technical controls that prevent the use of weak forms of MFA such as SMS and email.
    - There are higher password policy requirements for QHR employee accounts with privileged accesses. These are also enforced through technical controls.
    - Our password policy for the strength (complexity, length, reuse) of QHR employee passwords is enforced through technical controls.
    - There are a variety of other risk-based technical controls in place, such as preventing access where “impossible travel” logins are attempted.
- **Client Access**
    - Multi-factor authentication (MFA) is used for access to Accuro Cloud. QHR has technical controls that prevent the use of weaker forms of MFA such as SMS and email.
    - Our password policy for the strength of users' passwords is enforced through technical controls.
    - Accounts that aren't used for 60 days are automatically disabled.
    - The date, time, and IP address of all logins is recorded (in immutable logs).

b. Encryption

- QHR utilizes strong data encryption techniques and practices for PHI data and other critical data, both for data-at-rest and when in transit outside our data centers.
- Accuro data is encrypted using Microsoft SQL server transparent data encryption (TDE) which uses AES 256-bit encryption at rest.
- When PHI data is exchanged with our business partners it is encrypted in transit using TLS 1.2 or above with strong ciphers.
- When data is moved between our data centers (such as for backup purposes), the data at rest is encrypted and sent over an encrypted channel.

c. Event Logging and Retention

- QHR uses security information and event management (SIEM) where all logs from our environment are aggregated and used to detect anomalous and malicious behaviour within our entire environment. These logs are stored in Canada and retained for at least 2 years.
- QHR’s environment is monitored for security events 24x7x365 by a managed security service provider (MSSP).

d. Firewalls and Network Devices

- We employ firewalls with restrictive access control lists to protect our infrastructure. These are configured to only allow what we have explicitly allowed and deny anything else that has not been explicitly allowed by using a "Deny All" rule.
- Network devices, including firewall and other boundary devices, are in place to control and monitor communications at the external boundary of the network and at key internal boundaries within the network.

e. Security Awareness and Training

- We conduct regular phishing exercises to help teach employees to identify malicious emails.
- We employ protection on our email systems designed to minimize the possibility for phishing emails, or emails containing malware, to reach our employees.

f. Vulnerability Management and Penetration Testing

- QHR runs a vulnerability management program and conducts regular patching.
- QHR conduct various weekly and monthly automated scans of the security of our infrastructure.
- Penetration tests are conducted annually on our applications and infrastructure by a qualified independent third party.
- QHR uses Next-Generation Anti-Virus software across our environment to detect the most advanced and sophisticated attacks.

g. Other

- QHR employs security controls suitable to allow employees to work safely from outside of our offices while using a Zero Trust Network strategy.
- QHR maintains a list of high risk nations and blocks access accordingly.

2. Privacy & Data Residency

a. Privacy

- QHR has extensive experience in dealing professionally with the privacy issues and legislation surrounding health information. We work continuously to stay in compliance with the evolving Canadian federal and provincial requirements for privacy for the six provinces in which we operate. We have formal policies and procedures in place for handling privacy events.
- QHR has full time privacy staff and a designated Privacy Officer.
- Privacy awareness is integrated into QHR's employee onboarding process as well as in both initial and ongoing training programs.
- As per our License and Services Agreement, both parties are required to promptly notify each other of any breach of confidentiality or misuse of QHR or client confidential information. QHR will also report such incidents to the appropriate regulatory authorities when required.
- QHR's Privacy Policy is available at Privacy Policy - QHR Technologies

b. Data Residency

- Data is only stored long enough to complete the transaction is was collected for, or otherwise where QHR has a legitimate legal requirement.
- In the provision of our solutions, QHR manages (and in some cases hosts) personal information on behalf of healthcare providers, who remain the custodians of that personal health information.
- Personal Health Information (PHI) that QHR handles is stored in Canada in professionally-managed data centers.
- Personal Information (PI) that QHR handles is stored as described in our Privacy Policy - QHR Technologies under the 'Where do we Store Data' section.
- All backups of this data are also stored in Canada in professionally managed data centers.

3. Operational

a. Business Resilience

- QHR maintains a business continuity and disaster recovery plan that is invoked in the event of severe business interruptions. This is tested annually through table top exercises.

b. Data Recovery

- QHR has data architecture/design and practices that allow data to be recovered in the event of various data loss events. These events range from a disaster resulting in the loss of all data in a data center (fire, flood, etc.) to smaller losses such as major equipment failures. It also provides the ability to recover from more common events such as client or QHR mistakes that need to be rolled back.
- For Accuro, transaction logs of database activity are written live to a data center that is significantly physically distant (another province) from where the active database resides. This design is part of the measures we employ to achieve a goal to not lose more than the most recent 15 minutes of activity in the database. This is often called a Recovery Point Objective or RPO. We maintain these transaction logs for at least 10 days.
- The most recent full backup, or full backup plus subsequent incremental backups, are used together with the transaction logs to provide recovery of the data with minimal loss.
- Recovery of backups is tested and recorded quarterly.

c. Incident Management

- QHR maintains formalized incident management procedures to handle incidents that affect, or could affect, the normal operation of our systems and services.
- QHR's Status Page provides real-time updates and relevant information on incidents or downtime events affecting QHR products. This is the timeliest way to get information if your Accuro experience is affected. You can subscribe to receive Status Page notifications by text or email. To subscribe, visit: QHR Technologies Status Page Status.

d. System Availability and Maintenance Windows

- QHR's goal is to provide 99.9% availability of its Accuro and Accuro Engage/Medeo services excluding planned outages during maintenance windows.
- QHR publishes to the public the current availability of its key service offerings. You can see the current and historical availability at QHR Technologies Status Page Status.
- Planned outages that are outside of established maintenance windows are communicated to customers well ahead of time so they can take these into account in their own planning.

4. Compliance and Regulatory Frameworks

QHR undergoes multiple audits and assessments annually to ensure ongoing compliance with privacy and security standards. The table below outlines the key frameworks and certifications we adhere to.

Framework/ Regulation	Notes	Client Documentation
SOC 2 Type 2	SOC 2 Type 2 is a certification that evaluates how well an organization's systems and controls protect customer data over time. QHR undergoes an annual audit conducted by an independent third party to evaluate the effectiveness of our controls related to Security and Availability for AccuroEMR and Accuro Engage/Medeo products.	SOC 2 Summary: Accuro Resource Centre - Compliance at QHR Full SOC 2 report will require an NDA.
ISO 13485:2016 Quality Management System for Medical Device Manufacturing	ISO 13485:2016 is an international standard that outlines requirements for a Quality Management System (QMS) specific to medical devices. QHR maintains a Quality Management System (QMS) that governs the designing, developing, manufacturing, marketing, and servicing of the AccuroEMR software. QHR undergoes an annual audit audit conducted by an external certifying body to evaluate our QMS and maintain this certification.	ISO 13485: 2016 Medical devices QHR Technologies ISO13485 Certification.pdf
OntarioMD EMR Certification Program	Provincial body certifying that EMR vendors meet defined technical, functional, and regulatory requirements QHR's AccuroEMR product is verified and maintains compliance with OntarioMD's certification program.	Certified EMR Offerings OntarioMD Certification Program
Ontario Health's Virtual Visits Program	Provincial body that verifies and validates video and secure messaging solutions meet all mandatory requirements for privacy, security, technology, accessibility, and functionality. QHR's Accuro Engage product is verified and maintains compliance with Ontario Health's Virtual Visits requirements.	Verified Virtual Visit Solutions | Ontario Health
Payment Card Industry Data Security Standard (PCI:DSS)	PCI:DSS is a global organization ensuring that organizations meet standards for securely processing, storing, and transmitting credit card information. QHR maintains PCI DSS (Payment Card Industry Data Security Standard) SAQ A compliance to protect our client's credit card information.	Official PCI Security Standards Council Site
NIST Cybersecurity Framework (CSF) 2.0	The NIST Cybersecurity Framework (CSF) 2.0 provides guidelines to organizations to prevent, detect, and respond to cybersecurity risks.	NIST Cybersecurity Framework

	QHR conducts an annual security maturity assessment aligned with NIST to evaluate and strengthen our cybersecurity posture.	
ISO 14971:2019	ISO 14971 is an international standard that outlines requirements for identifying, evaluating, controlling, and monitoring risks associated with medical devices throughout their lifecycle. QHR's Risk Management Framework is aligned with the principles and structure of this standard.	ISO 14971:2019
Personal Information Protection and Electronic Documents Act (PIPEDA)	Canadian federal privacy law governing how private-sector organizations collect, use, and disclose personal information in the course of commercial activities. QHR's privacy practices and Privacy Impact Assessments are based on this framework.	Accuro PIA Supporting Information
Provincial Privacy Laws and Regulations	QHR Technologies complies with all applicable Canadian privacy laws and regulations in the provinces in which we operate.	Accuro Resource Centre - Privacy and Security

5. Additional Resources

- QHR Technologies Inc. Privacy Policy: Privacy Policy - QHR Technologies
- QHR's Terms of Use: Terms of Use - QHR Technologies
- Accuro Resources - Compliance: Accuro Resource Centre
- Accuro Resources - Privacy & Security: Accuro Resource Centre

6. Version History

Version	Date	Contributors	Comments
1.0	2021-07-23	Arnold Nzailu, Senior Information Security Officer Aron Ashmead, Privacy Officer Alan McNaughton, Director of Technology Operations Stephanie Smith, GRC Manager Jerry Diener, Senior Director of Corporate Development Crystal Benoit, GRC Team Lead	Release Version.
2.0	2022-04-11	Alan McNaughton, Director of Technology Operations Aron Ashmead, Privacy Officer	Corrected data residency of PI.
2.1	2023-09-18	Crystal Benoit, GRC Manager	Removed 'confidential' classification.
3.0	2025-09-08	Alan McNaughton, Director of Technology Operations Alison Moore, Quality Audit Specialist Crystal Benoit, Sr. Manager, Governance, Risk and Compliance Ronald Lai, Compliance Specialist	Overall reorganization/update of information, retracted name of MSSP, added business continuity plan, added table of contents, added compliance frameworks section